Principes applicables à tous les services de confiance et au document électronique

Jacquemin, Hervé

Published in:
L'identification électronique et les services de confiance depuis le règlement eIDAS

Publication date:
2016

Document Version
le PDF de l'éditeur

Principes applicables à tous les services de confiance et au document électronique

Hervé JACQUEMIN*

Introduction

1.- Des services de confiances pour lever les obstacles formels. Les technologies de l'information et de la communication constituent désormais une réalité quotidienne, notamment en matière contractuelle. On constate néanmoins que les exigences de forme sont légions, qu'elles soient requises à des fins probatoires ou constituent des conditions de validité du contrat. Les contrats imprimés sur le papier, au bas desquels chaque partie appose sa signature manuscrite, sont ainsi remplacés, de plus en plus souvent, par des documents électroniques, transmis par courriels et munis – mais très rarement – d'une signature électronique. Par ailleurs, on observe une volonté certaine des entreprises ou des autorités publiques d'aller vers davantage de dématérialisation, pour simplifier les procédures et diminuer les coûts de traitement et de conservation.

Encore faut-il s'assurer qu'il est légalement permis de recourir à des procédés électroniques pour accomplir l'exigence de l'écrit, de la signature, des mentions manuscrites, voire pour envoyer un recommandé ou archiver les documents, de sorte que ces formalités auront les mêmes effets, sur le plan juridique, que les exigences correspondantes dans l'environnement papier.

Dans un environnement ouvert (où les parties ne se connaissent pas nécessairement), l'intervention d'un tiers de confiance a paru requise pour lever certains obstacles formels. Aussi le législateur est-il intervenu pour encadrer les activités de ces prestataires et les services fournis par ceux-ci : c'est le cas pour la signature électronique (depuis 1999 en droit de l'UE) et, désormais, pour le cachet, le recommandé et l'horodatage électroniques, ainsi que l'authentification de sites internet. Pour les autres formalités (document électronique, écrit ou mentions manuscrites),

* Chargé d'enseignement à l'Université de Namur (CRIDS), chargé de cours invité à l'UCL et à l'ICHEC, avocat au barreau de Bruxelles.

la sécurité juridique peut être garantie sans l'intervention d'un tiers de confiance, mais moyennant la consécration de principes directeurs, applicables par ailleurs aux autres services de confiance.

2.- Cadre normatif limité à la signature électronique. Le législateur est intervenu très – sans doute même trop – tôt en matière de signature électronique. Au niveau international, on se rappelle ainsi des lois-types de la CNUDCI sur le commerce électronique (1996) et sur la signature électronique[1] (2001), ainsi que des directives européennes sur la signature électronique[2] (1999) et sur le commerce électronique[3] (2000).

En droit belge, les principales dispositions légales sont en vigueur depuis le début des années 2000. Pour la signature, il faut principalement avoir égard à l'article 1322, alinéa 2, du Code civil[4] et à la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électronique et les services de certification[5] (qui transposent la directive sur la signature électronique). Il faut également mentionner les articles 16 et 17 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information[6] (LSSI), désormais intégrés dans le livre XII du Code de droit économique (art. XII.15 et XII.16), qui consacrent la théorie des équivalents fonctionnels et l'appliquent à l'écrit, la signature et la mention manuscrite.

Parmi les services de confiance, seule la signature électronique fait ainsi l'objet d'un régime spécifique.

3.- Quid des autres services de confiance ? Des initiatives avaient toutefois été prises, par le législateur belge, pour réguler d'autres services de confiance.

Une loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance[7] a ainsi été adoptée mais, en l'absence

[1] On peut également ajouter la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005). Ces textes sont disponibles sur le site web de la CNUDCI (www.uncitral.org).

[2] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, *J.O.*, L. 13 du 19 janvier 2000.

[3] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.*, L. 178 du 17 juillet 2000.

[4] Cet alinéa 2 a été ajouté par l'art. 2 de la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000.

[5] *M.B.*, 29 septembre 2001.

[6] *M.B.*, 17 mars 2003.

[7] *M.B.*, 17 juillet 2007.

d'arrêté royal complétant le dispositif, le régime est inutilisable. Cette loi encadre les activités des prestataires de service d'archivage électronique, d'horodatage électronique, de recommandé électronique et de blocage transitoire des sommes versées. Diverses obligations, assez générales, sont imposées à ces prestataires. Elles portent sur leur impartialité (art. 4), leur attitude vis-à-vis des données qui leur sont transmises (art. 5), les mesures de sécurité à mettre en œuvre (art. 6), les informations à communiquer aux destinataires de leurs services (art. 7), la compétence de leur personnel (art. 8), la confidentialité (art. 9) et leur capacité financière (art. 10). Pour le surplus, la loi donne délégation au Roi pour déterminer, par arrêté délibéré en conseil des ministres, les obligations spécifiques auxquelles est soumis chacun des prestataires visés par la loi (art. 16, al. 1er, 1°). L'article 16 impose au Roi d'intervenir jusqu'au 1er décembre 2007 au plus tard. Il apparaît cependant qu'il n'est jamais intervenu.

Plus récemment, les services d'archivage, d'horodatage et de recommandé électroniques ont également fait l'objet d'une proposition de loi[8]. Elle visait à introduire dans le livre XII du Code de droit économique (intitulé « droit de l'économie électronique ») un titre 2 reprenant les dispositions de la loi du 9 juillet 2001 et de nouvelles dispositions sur ces trois services de confiance. Dans le cadre de la procédure instaurée par la directive « transparence »[9], le texte avait été bloqué par la Commission jusqu'en octobre 2014 (tenant compte de l'adoption prévue du règlement eIDAS), soit après les élections législatives de mai 2014. Aussi la proposition est-elle devenue caduque.

On note encore que l'envoi recommandé est déjà défini à l'article 131, 9°, de la loi du 21 mars 1991 portant réforme de certaines entreprises

[8] Proposition de loi du 15 avril 2013 modifiant la législation en ce qui concerne l'instauration du droit de l'économie électronique, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 2745/001. Voy. aussi l'amendement du Gouvernement visant à compléter la proposition de loi portant insertion d'un titre 2, 'Certaines règles relatives au cadre juridique pour les signatures électroniques, l'archivage électronique, le recommandé électronique, l'horodatage électronique et les services de certification', dans le livre XII du Code de droit économique, et portant insertion des définitions propres au titre 2 précité et des dispositions d'application de la loi propres au même titre, dans les livres I et XV du Code de droit économique, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 2745/004.

[9] Directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.*, L. 204 du 21 juillet 1998. Depuis lors, cette directive a été abrogée et remplacée par la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.*, L. 241 du 17 septembre 2015.

publiques économiques[10], comme « un service garantissant forfaitairement contre les risques de perte, vol ou détérioration et fournissant à l'expéditeur, le cas échéant à sa demande, une preuve de la date du dépôt de l'envoi postal et/ou de sa remise au destinataire ». Nonobstant son importance pratique considérable, l'incertitude restait cependant de mise quant à la valeur légale des procédés de recommandé électronique. Conformément à l'article 135, § 2, de la loi du 21 mars 1991, « toutes les obligations reprises dans la présente loi et dans toutes les autres lois relatives aux matières visées à l'article 78 de la Constitution et leurs arrêtés d'exécution qui, concernant les envois recommandés, contiennent les mots "à la poste", "par la poste" ou toute autre référence du même type sont remplies lorsqu'est utilisé un envoi recommandé tel que défini à l'article 131, 9° de la présente loi ou un envoi recommandé électronique conformément à la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques, le recommandé électronique et les services de certification ». Le renvoi à la loi du 9 juillet 2001 est cependant erroné, toute référence au recommandé ayant été supprimée[11].

4.- Règlement eIDAS. Après 15 ans, constatant que le cadre normatif applicable à la signature électronique demeurait très perfectible (eu égard, notamment, aux différences constatées entre les États membres) et qu'il restait de nombreuses incertitudes pour diverses formalités, sans doute accessoires, mais néanmoins cruciales en pratique (en matière d'horodatage ou de recommandé électroniques, par exemple), le législateur européen a remis l'ouvrage sur le métier.

Aussi la Commission a-t-elle pris l'initiative et déposé une proposition de règlement en juin 2012[12]. Le texte a été adopté près de deux ans plus tard : il s'agit du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les

[10] *M.B.*, 27 mars 1991.

[11] La loi du 13 décembre 2010 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges et modifiant la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (*M.B.*, 31 décembre 2010) encadrait les services de recommandé électronique et déterminait les conditions dans lesquelles le procédé mis en place pouvait être jugé équivalent au procédé traditionnel de la lettre recommandée à La Poste, en introduisant diverses dispositions dans la loi du 9 juillet 2001. Cette loi du 13 décembre 2010 a cependant été abrogée avec effet immédiat par une loi du 31 mai 2011 portant des dispositions diverses en matière de télécommunication (*M.B.*, 21 juin 2011).

[12] Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, 4 juin 2012, COM (2012) 238 final.

services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[13] (ci-après, « règlement eIDAS »)[14].

On aura aussi égard, de manière ponctuelle, à l'avant-projet de loi belge qui met en œuvre le règlement eIDAS et complète le titre 2 du livre XII du Code de droit économique (« certaines règles relatives au cadre juridique pour les services de confiance »)[15].

5.- Objet et plan de la contribution. L'encadrement, dans un même instrument juridique (le règlement eIDAS), de plusieurs services de confiance, n'a de sens que si ces services sont soumis, dans la mesure du possible, à un régime cohérent et harmonisé. À l'analyse, tel est effectivement le cas, en ce sens que l'on peut dégager des principes communs à tous les services de confiance visés par le règlement.

L'objectif de la présente contribution est d'examiner ceux-ci, étant entendu que chaque service de confiance – signature, cachet, horodatage et recommandé électroniques – sera ensuite analysé de manière détaillée dans d'autres titres de l'ouvrage[16]. Seule l'authentification de site internet ne fera pas l'objet d'une contribution à part entière, compte tenu du régime très limité dont elle fait l'objet.

Nous nous pencherons aussi sur le document électronique. Il ne constitue pas un service de confiance en tant que tel mais est soumis au principe de non-discrimination (à l'instar des autres services de confiance). Nous l'étudierons donc dans ce contexte.

Après avoir rappelé l'acception des principales notions, tout en pointant les éléments permettant de cerner le domaine d'application du règlement (Chapitre 1), nous voyons dans quelle mesure il consacre, de

[13] *J.O.*, L. 257 du 28 août 2014.

[14] Pour une première analyse du règlement, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution », *R.D.T.I.*, 2014/56, pp. 27 et s. ; H. JACQUEMIN, « Preuve et services de confiance dans l'environnement numérique », in *Pas de droit sans technologie*, CUP, vol. 158, Bruxelles, Larcier, 2015, pp. 41 et s.

[15] Avant-projet de loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique.

[16] Nous renvoyons à la contribution de B. Losdyck pour la signature électronique, à celle de J.-B. Hubin pour le cachet électronique et à celle de Ch. Verdure pour l'horodatage et le recommandé électroniques.

manière expresse ou implicite, certains principes directeurs (Chapitre 2), avant de distinguer les règles en matière de services qualifiés et de services non-qualifiés (Chapitre 3).

CHAPITRE I. Notions et domaine d'application

6.- Objet du règlement eIDAS et domaine d'application. L'objet du règlement eIDAS est énoncé en son article 1er : il « a) fixe les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre ; b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques ; et c) instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, d'envoi recommandé électronique et les services de certificats pour l'authentification de site internet ».

En l'occurrence, seuls les points b) et c) retiennent notre attention. Ces éléments sont principalement visés par le chapitre III du règlement eIDAS sur les services de confiance. On ajoutera le chapitre IV sur le document électronique.

Le champ d'application de ces dispositions doit être circonscrit à la lumière des notions utilisées, telles que définies à l'article 3 (*infra*, n° 7), tout en tenant compte des limites posées, notamment, à l'article 2 (*infra*, n° 8) du règlement eIDAS.

7.- Notions de « services de confiance (qualifié) » et de « prestataire de service de confiance (qualifié) ». Au sens du règlement eIDAS, le prestataire de confiance est « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié »[17]. Le prestataire de service de confiance qualifié est également défini : le règlement désigne ainsi « un prestataire de service de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut de qualifié »[18]. Deux conditions, tenant à la nature du service fourni et à l'autorisation administrative dont le prestataire a fait l'objet, se dégagent ainsi de cette définition. Nous les examinerons par la suite (*infra*, nos 25 et s.).

[17] Art. 3, 19°, du règlement.

[18] Art. 3, 20°, du règlement.

Le service de confiance est quant à lui « un service électronique normalement fourni contre rémunération qui consiste :

a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou

b) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou

c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services »[19].

À l'instar des « services » (au sens de la directive 2006/123/CE ou des articles 56 et 57 du Traité sur le fonctionnement de l'Union européenne), des « services de la société de l'information » (au sens de la directive 2000/31/CE) ou des « services de médias audiovisuels (au sens de la directive 2010/13/EU), le service de confiance doit être « normalement fourni contre rémunération ». Suivant la jurisprudence de la Cour de justice de l'Union européenne à ce sujet, l'exigence d'une rémunération signifie qu'une contrepartie économique doit exister. On note que la poursuite d'un but de lucre n'est pas une condition de l'existence d'un service au sens du Traité ; le prestataire de services peut donc être une ASBL. En outre, il n'est pas requis que la contrepartie soit payée directement au prestataire par le destinataire[20]. Répond ainsi à la définition du service une prestation fournie gratuitement à ce dernier mais dont le financement est assuré par des tiers, moyennant des recettes publicitaires, par exemple. La précision est importante : sur l'internet, il s'agit en effet du modèle économique retenu par de nombreux sites web et rien n'empêche que les prestataires de service de confiance recourent également à ce modèle[21]. Les activités financées par les pouvoirs publics ou fournies par une entité publique n'échappent pas nécessairement à la notion, pour autant que la contrepartie économique demeure et qu'elles ne s'inscrivent pas dans la mission de service public de l'autorité[22].

[19] Art. 3, 16°, du règlement.

[20] C.J.C.E., 12 juillet 2001, C-157/99, *Smits et Peerbooms*.

[21] Dans l'arrêt *Papasavvas* du 11 septembre 2014, la Cour de justice de l'Union européenne a confirmé que cette notion « englobe des services fournissant des informations en ligne pour lesquels le prestataire est rémunéré non pas par le destinataire, mais par des revenus générés par des publicités diffusées sur un site internet » (C.J.U.E., 11 septembre 2014, aff. C-291/13, *Papasavvas*, pt 30).

[22] En ce sens, voy. le considérant n° 34 de la directive 2006/123/CE sur les services. On peut y lire que « La Cour de justice a estimé que la caractéristique essentielle de la rémunération réside dans le fait que celle-ci constitue la contrepartie économique des services en cause et que cette caractéristique est absente dans le cas des activités qui sont accomplies,

On aura noté que l'archivage électronique ne figurait pas parmi les services de confiance encadrés par le règlement, ce qui est regrettable[23]. Tout au plus est-il visé à la marge, au point c) de la définition du service de confiance, pour la conservation des signatures électroniques, des cachets électroniques ou des certificats relatifs à ces services (voy. aussi les articles 34 et 40 du règlement eIDAS).

Le service de confiance qualifié » est également défini par le règlement, mais de manière curieuse et, en tout état de cause, peu utile dans une perspective de qualification : il s'agit en effet du « service de confiance qui satisfait aux exigences du présent règlement »[24].

Pour une analyse détaillée de chaque service de confiance, nous renvoyons aux autres contributions de cet ouvrage.

8.- Domaine d'application du règlement eIDAS. L'article 2 du règlement pose deux limites à son domaine d'application.

Le règlement ne « s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants »[25]. Le considérant n° 21 du règlement donne l'exemple des « systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance [qui] ne devraient pas être soumis aux exigences du présent règlement », tout en précisant que « seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement ». Dans ces hypothèses, les prestataires ne sont pas tenus de recourir à des services de confiance. Sur le plan des principes, cette exclusion paraît logique : dans un système fermé où, normalement, les parties se connaissent (et ont encadré leur relation par l'adoption de dispositions contractuelles), il n'est pas requis de recourir à un tiers de confiance. Conformément au principe de la liberté contractuelle, les parties pourraient donc décider,

sans contrepartie économique, par l'État ou pour le compte de l'État, dans le cadre de ses missions dans les domaines social, culturel, éducatif et judiciaire, tels que les cours dispensés au sein du système d'éducation nationale ou encore la gestion des régimes de sécurité sociale qui n'ont aucune activité de nature économique. Les montants versés par les destinataires à titre de participation aux frais de fonctionnement d'un système, par exemple les frais d'inscription ou de scolarité payés par les étudiants, ne constituent pas en eux-mêmes une rémunération dans la mesure où le service est toujours essentiellement financé par des fonds publics. Ces activités ne sont donc pas couvertes par la définition de « service » à l'article 50 du traité et n'entrent donc pas dans le champ d'application de la présente directive ».

[23] Sur ce point, voy. la contribution d'O. Vanreck dans le présent ouvrage.

[24] Art. 3, 17°, du règlement.

[25] Art. 2, § 2, du règlement.

conventionnellement, de reconnaître des effets juridiques à un procédé de signature électronique ou d'horodatage électronique qui ne satisfait pas aux conditions du règlement. La pratique est courante dans les règlements des opérations établis par les banques[26] ou, de manière générale, pour ce qui est des formalités probatoires telles que régies par le Code civil (dont le régime n'est ni impératif, ni d'ordre public). Cette manière de faire est parfaitement licite – et sort du domaine d'application du règlement – pour autant que cette convention ne méconnaisse aucune autre disposition légale ou réglementaire applicable par ailleurs. Ainsi, dans un contrat entre une entreprise et un consommateurs, la clause devrait être jugée abusive si elle a pour objet de « limiter de manière non autorisée les moyens de preuve que le consommateur peut utiliser ou lui imposer une charge de la preuve qui incombe normalement à une autre partie au contrat »[27]. De même, si la loi impose une signature manuscrite ou électronique qualifiée et qu'il s'agit d'une condition de validité du contrat[28], les parties ne pourraient normalement pas s'entendre pour recourir à un procédé de signature électronique simple ; en tout état de cause, l'exigence n'échappe pas au champ d'application du règlement sur le fondement de l'article 2, § 2.

S'agissant spécialement des services de confiance, le règlement ne limite pas son application aux hypothèses dans lesquelles les formalités seraient requises dans une perspective probatoire ou pour d'autres finalités, telles les exigences requises *ad validitatem*. Peu importe également que les services de confiance soient utilisés dans le secteur privé ou dans le secteur public, de manière transfrontalière ou purement nationale[29]. Par

[26] Dans le Règlement général des opérations d'une banque, on peut ainsi lire que « le Client accepte que les données informatiques/électroniques enregistrées par la Banque font preuve des opérations ainsi que des ordres, avis ou information échangés par voie électronique, quel que soit le support sur lequel ces données sont enregistrées. Pour ces opérations électroniques, la signature électronique du Client remplace la signature manuscrite ». Il est ensuite précisé les procédés qui peuvent être considérés comme une signature électronique. Il s'agit notamment de l'introduction d'un code pin, d'un code secret, d'un code d'accès, voire de la combinaison de l'introduction d'une carte bancaire ou de crédit avec un code personnel.

[27] Art. VI.83, 21°, CDE.

[28] Comme en matière de crédit à la consommation, par exemple (voy. en ce sens l'art. VII.78 du Code de droit économique). Sur ce point, voy. la contribution de H. Jacquemin et de C.R. Joly, dans le présent ouvrage.

[29] Pour l'identification électronique, le règlement va moins loin puisqu'il se focalise sur les hypothèses d'e-gouvernement (le secteur privé étant par ailleurs encourager à utiliser les moyens d'identification, sur une base volontaire – *cf.* le considérant n° 17) et l'utilisation des moyens d'identification électronique dans une perspective transfrontalière. Pour une comparaison entre les dispositions du chapitre II et du chapitre III du règlement, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution », *op. cit.*, pp. 31 et s.

contre, le règlement eIDAS « n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel »[30] (art. 2, § 3). Deux éléments doivent être distingués : l'exigence formelle en tant que telle, prescrite par un texte légal ou réglementaire (la signature requise en matière probatoire, conformément à l'article 1341 du Code civil), d'une part, l'effet juridique reconnu au procédé susceptible d'être mis en œuvre dans l'environnement numérique, d'autre part. Le règlement ne s'applique qu'au second aspect, laissant aux États membres le soin de déterminer quelles exigences formelles sont requises, leurs finalités et les sanctions susceptibles d'être prononcées en cas de non-respect.

CHAPITRE II. Principes directeurs

9.- Trois principes directeurs. Au moment de lever les obstacles formels, trois principes directeurs sont généralement consacrés – ou, à tout le moins, mis en œuvre – par le législateur : le principe de non-discrimination, le principe d'équivalence fonctionnelle et la neutralité technologique.

Nous revenons sur chacun d'eux et examinons de quelle manière ils sont traités dans le règlement eIDAS.

SECTION 1. – Principe de non-discrimination

10.- Directives antérieures à eIDAS et droit belge. Conformément l'article 9, § 1er, de la directive sur le commerce électronique, « les États membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les États membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise

[30] On trouvait une exigence comparable à l'article 1er de la directive 1999/93/CE sur la signature électronique : « Elle ne couvre pas les aspects liés à la conclusion et à la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire ; elle ne porte pas non plus atteinte aux règles et limites régissant l'utilisation de documents qui figurent dans la législation nationale ou communautaire ».

à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique ».

On ne trouve pas, en droit belge, de consécration générale de ce principe de non-discrimination, applicable à toutes les formalités. On trouve certes un énoncé du principe d'équivalence fonctionnelle[31] et des clauses transversales d'assimilation pour les formalités les plus fréquentes (écrit, signature et mention manuscrite)[32] mais leur champ d'application est limité par l'article XII.16 et exclut notamment les sûretés (on ne peut donc pas l'invoquer pour les actes de cession de rémunération, visés à l'article 27 de la loi du 12 avril 1965, par exemple[33]). Cela dit, les formalités couvertes par les clauses d'assimilation bénéficient à tout le moins du principe de non-discrimination. Qui peut le plus peut le moins.

Pour transposer la directive sur la signature électronique, le principe a toutefois été consacré à l'article 4, § 5, de la loi du 9 juillet 2001 sur la signature électronique et les PSC, qui stipule qu' « une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif [...] que la signature se présente sous forme électronique [...] »[34]. À ce principe est par ailleurs associé le principe d'assimilation, étroitement lié à l'application de la théorie des équivalents fonctionnels[35].

11.- Règlement eIDAS. Dans le règlement eIDAS, le principe de non-discrimination est appliqué aux services de confiance (§ 1) et au document électronique (§ 2).

§ 1. Services de confiance

12.- Consécration du principe de non-discrimination pour les services de confiance. Le règlement applique expressément le principe

[31] Art. XII.15, § 1er, CDE.

[32] Art. XII.15, § 2, CDE.

[33] À ce sujet, voy. la contribution de H. Jacquemin et de C.-R. Joly, dans le présent ouvrage.

[34] On note que cette disposition transpose littéralement l'article 5, § 2, de la directive sur la signature électronique.

[35] Sur ces deux principes, voy. not. E. Montero, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *D.A.O.R.*, 2002, pp. 13 et s. ; D. Gobert et E. Montero, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, pp. 116-117 ; P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *Le commerce électronique : un nouveau mode de contracter*, Liège, Éd. du Jeune Barreau, 2001, pp. 106 et s. ; M. Antoine et D. Gobert, « La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet ? », *J.T.D.E.*, 2000, pp. 74-75, nos 5-8.

de non-discrimination à la signature électronique[36], au cachet électronique[37], à l'horodatage électronique[38] et au service d'envoi recommandé électronique[39], en interdisant notamment que l'effet juridique et la recevabilité comme preuve en justice leur soient refusés au seul motif qu'ils se présentent sous forme électronique ou que le service n'est pas qualifié.

L'interdiction de toute discrimination s'applique ainsi au bénéfice d'un service de confiance qualifié (par rapport à un service non qualifié) et au bénéfice d'un service de confiance – par définition de nature électronique – par rapport à un procédé correspondant dans l'environnement papier (une signature manuscrite, par exemple). Cette double déclinaison du principe de non-discrimination ne repose pas sur le même objectif.

Dans le premier cas, le législateur intervient sur le marché des services de confiance qui, comme on le sait, peuvent être qualifiés et non qualifiés. Les services de confiances qualifiés sont soumis à des conditions très lourdes mais, en contrepartie, les effets qui leur sont attachés offrent un niveau de sécurité juridique plus élevé (*infra*, n^{os} 26 et s.). Le législateur est néanmoins conscient que, suivant l'hypothèse concernée, il ne faut pas nécessairement disposer d'un service qualifié. Autrement dit, il existe un marché pour les services qualifiés et un marché pour les services non qualifiés. Aussi interdit-il que tout effet juridique leur soit refusé au seul motif que le service de confiance n'est pas qualifié. La liberté des parties de recourir à un service plutôt qu'à l'autre est ainsi préservée.

Dans le second cas, c'est la dématérialisation des échanges, et le recours aux technologies de l'information et de la communication dans les transactions électroniques, que le législateur entend défendre. Le règlement eIDAS perdrait tout effet utile si, en cas de litige, la juridiction pouvait tout simplement refuser d'examiner le procédé (un procédé de signature électronique appliqué à un courriel, par exemple) au seul motif qu'il est électronique.

13.- Portée du principe de non-discrimination. Plusieurs précisons peuvent être apportées pour cerner correctement la portée du principe de non-discrimination.

Elles concernent d'abord l'articulation (et la différence) entre le principe de non-discrimination et les clauses d'assimilation ou les présomptions d'équivalence (*infra*, n° 14) ainsi que l'application du principe à d'autres domaines que la preuve (*infra*, n° 15).

[36] Art. 25, § 1er, du règlement.
[37] Art. 35, § 1er, du règlement.
[38] Art. 41, § 1er, du règlement.
[39] Art. 43, § 1er, du règlement.

Nous traiterons aussi de la question de savoir si ce principe empêche le législateur national d'imposer une signature électronique qualifiée, ou tout autre service de confiance qualifié, à l'exclusion d'une signature non qualifiée ou d'un autre service de confiance non qualifié (*infra*, n° 16).

14.- Distinction entre la non-discrimination et l'assimilation (ou la reconnaissance d'effets équivalents). On note d'abord que l'interdiction de priver d'effet juridique un service de confiance au seul motif qu'il est accompli par voie électronique ne signifie pas qu'il est, *ipso facto*, jugé équivalent au procédé correspondant dans l'environnement papier (avec les mêmes effets juridiques). Pour tirer cette conclusion, il faut poursuivre l'analyse et démontrer que les fonctions de la formalité, telles qu'énoncées par le législateur, ou identifiées par l'interprète, ont été atteintes (le cas échéant, en se basant sur une clause d'assimilation ou une présomption établie légalement, comme le fait le règlement eIDAS avec les services de confiance qualifiés).

Un raisonnement en deux temps doit ainsi être accompli : non-discrimination *certaine* dans un premier temps avec, dans un second temps, la *possible* reconnaissance d'une équivalence avec le procédé traditionnel ou du respect des fonctions attendues du procédé.

Cette manière de faire n'est pas sans poser de question ou, en tout cas, elle peut paraître très artificielle, tenant compte de l'examen auquel doit se livrer le magistrat saisi d'un litige.

L'affirmation du principe de non-discrimination peut se comprendre si on envisage la formalité – par exemple la signature – dans une perspective probatoire. On sait en effet que la méconnaissance des règles de preuve se traduit, sur le terrain de la sanction, en termes de recevabilité et de valeur (ou de force) probante. On peut concevoir qu'un moyen de preuve soit recevable (principe de non-discrimination) mais ne possède pas de force probante et qu'aucune valeur probante ne lui soit reconnue (inapplication en l'espèce de la présomption d'équivalence ou de la clause d'assimilation).

Par contre, s'agissant des formalités qui ne sont pas requises (uniquement) dans une perspective probatoire (des formalités requises *ad validitatem*, par exemple), il n'y a pas de sanction intermédiaire. Par exemple, en l'absence de signature valable, l'acte juridique est nul ou converti. Le principe de non-discrimination n'a pas vraiment d'intérêt : ce qui importe, c'est de savoir si la signature électronique est assimilée à une signature manuscrite. À défaut, la sanction doit en principe être appliquée. Le raisonnement en deux temps présente cependant l'avantage d'obliger le magistrat à examiner le procédé litigieux et, sur le plan pédagogique, il conserve un intérêt certain.

15.- L'application du principe de non-discrimination n'est pas limitée aux formalités probatoires. Les termes utilisés dans les clauses de non-discrimination du règlement eIDAS applicables aux services de confiance pourraient être de nature à instiller le doute : s'agissant de la signature, par exemple, il est stipulé que « l'effet juridique et la recevabilité *d'une signature électronique* comme preuve en justice ne peuvent pas être refusés au seul motif que... » (nous soulignons). Sans doute la disposition aurait-elle été plus claire si elle avait prévu – comme dans les autres versions linguistiques, que « l'effet juridique et la recevabilité comme preuve en justice *d'une signature électronique*... ».

Il n'en reste pas moins, que, comme sous l'empire de la directive sur la signature électronique, la recevabilité comme preuve en justice doit être vue comme une hypothèse, parmi d'autres, de l'effet juridique de la signature électronique (ou du service de confiance).

L'article 4, § 5, de la loi du 9 juillet 2001 prévoit qu' « une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif [...] que la signature se présente sous forme électronique [...] »[40]. À ce propos, la doctrine avait considéré, avec raison, que le refus de la signature comme preuve en justice, devait être considéré comme une application particulière de l'inefficacité juridique, qui recouvre également d'autres sanctions (la nullité de l'acte juridique pour défaut de signature, par exemple)[41].

16.- La clause de non-discrimination s'impose-t-elle au législateur ? On peut se demander si la clause de non-discrimination s'impose uniquement aux juridictions chargées d'apprécier les effets juridiques des procédés qui lui sont soumis ou si elle s'impose aussi au législateur, lui interdisant de prescrire l'accomplissement de formalités qui ne peuvent être exécutées que dans l'environnement papier ou le recours à un service de confiance qualifié (à l'exclusion d'un service non qualifié).

S'agissant de la discrimination électronique/papier, la réponse est normalement assez claire : l'objectif du législateur est de *permettre* et *encourager* le recours aux technologies de l'information pour accomplir les exigences formelles, avec des services présentant un niveau plus ou moins élevé de sécurité technique et juridique, pas d'*imposer* le tout électronique. Dans de nombreuses hypothèses, il reste en effet justifié de recourir à des

[40] On note que cette disposition transpose littéralement l'article 5, § 2, de la directive sur la signature électronique.

[41] Considérant que, nonobstant la formulation de la loi, l'irrecevabilité est une hypothèse, parmi d'autres, de l'inefficacité juridique, voy. P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *op. cit.*, pp. 109-111 ; L. Guinotte, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, 2002, p. 559.

formalités « papier », spécialement lorsqu'elles requièrent l'intervention d'un tiers (un notaire, par exemple). Tel était d'ailleurs le sens de l'article 9 de la directive sur le commerce électronique, qui excluait diverses matières de l'obligation de lever les obstacles formels.

Mutatis mutandis, on devrait normalement tenir le même raisonnement pour la discrimination services qualifiés/services non-qualifiés, puisqu'ils se trouvent dans une seule et même clause. On se rappellera néanmoins que les objectifs poursuivis ne sont pas les mêmes (*supra*, n° 12). Aussi sommes-nous tenté de penser que, pour ce cas de figure, le législateur doit en tout cas s'efforcer de respecter l'esprit de la règle. En ce sens, nous croyons que le choix d'imposer uniquement un service de confiance qualifié doit se faire à l'aune des critères généralement mis en œuvre pour considérer qu'une restriction à une libre prestation de service, au sens de l'article 56 du Traité sur le fonctionnement de l'Union européenne, est légalement permise. Autrement dit, il faut s'assurer que l'exigence d'une signature électronique qualifiée (à l'exclusion d'une signature électronique non-qualifiée), par exemple, est justifiée par une raison impérieuse d'intérêt général (la protection des consommateurs, par exemple), qu'elle est propre à garantir la réalisation du ou des objectifs avancés par le législateur et qu'elle ne va pas au-delà de ce qui est nécessaire pour l'atteindre. En tout état de cause, ces restrictions doivent être appliquées de manière non discriminatoire.

Aussi s'étonne-t-on des dispositions générales figurant dans l'avant-projet de loi, et qui semblent exiger un envoi recommandé électronique qualifié, un service d'archivage électronique qualifié ou un service d'horodatage électronique qualifié lorsque le destinataire du service opte pour la voie électronique et qu'un envoi recommandé, une obligation de conservation ou une obligation de datation est imposé de manière expresse par un texte légal ou réglementaire (futur art. XII.25, §§ 5, 7 et 8, du CDE). Une analyse au cas par cas devrait être réalisée, pour s'assurer que, dans le cas d'espèce visé, la sécurité juridique et technique offerte par le procédé est indispensable (sauf à considérer que, par ailleurs, le législateur reverra le cadre normatif dans son ensemble, pour préciser, au cas par cas, s'il faut un service de confiance qualifié ou pas – ces dispositions valent en effet « sous réserve de l'application d'exigences légales ou réglementaires particulières).

De même, pour la conclusion d'un contrat de crédit à la consommation par voie électronique, l'article VII.78, § 1er, du Code de droit économique impose une signature électronique qualifiée ou une signature électronique qui répond à certains critères fixés par le Roi. Imaginons qu'aucun arrêté royal ne soit jamais adopté ou qu'il impose des exigences particulièrement lourdes (et finalement très proches de celles de la signature électronique qualifiée). Il s'agit assurément d'une restriction à la liberté

des consommateurs de recevoir les services d'un prestataire de service de confiance non-qualifié (susceptible de lui offrir un service de signature électronique). En l'occurrence, le législateur la justifiera probablement par l'objectif de protection des consommateurs (avec le risque de surendettement de comporte la conclusion d'un contrat de crédit). On comprend que, si la signature électronique n'est pas qualifiée, le risque existe que le consommateur qui signe le contrat de crédit ne soit pas celui qu'il prétend être (puisque le procédé présente *a priori* moins de garanties sur le plan de l'authenticité de l'origine). Dans ce cas cependant, sans doute le procédé aurait-il également été rejeté par le juge conformément à l'article 1322, alinéa 2, du Code civil (qui n'est toutefois pas applicable en matière de crédit à la consommation dès lors qu'il existe des dispositions spécifiques en matière de signature électronique). En outre, il s'agit ici de trouver un équivalent fonctionnel à la signature manuscrite du consommateur (dont les garanties offertes en termes d'authenticité de l'origine sont très faibles – et ne parlons même pas de l'identification du signataire, la plupart des signatures manuscrites étant tout simplement illisibles). D'ailleurs, pour s'assurer de l'identité du consommateur (qui est effectivement cruciale en matière de crédit, en lien avec la consultation de la centrale de crédits aux particuliers), l'article VII.76 du Code de droit économique exige du prêteur qu'il vérifie les données d'identification du consommateur sur la base, notamment, de sa carte d'identité. La carte d'identité électronique belge permet de procéder à cette vérification (à condition de recourir au service d'authentification – et pas de signature – qu'elle contient). Si le prêteur est une institution bancaire qui a par ailleurs vérifié l'identité de son client, et a pris l'habitude de l'authentifier au moment d'un digipass, par exemple, nous ne voyons pas d'objection à ce que la vérification soit réalisée de cette manière[42]. En réalité, c'est sur le prêteur que repose le risque : le consommateur pourrait en effet prétendre que le contrat de crédit n'a pas été valablement signé, en méconnaissance de l'article VII.78 et de l'article VII.90 du Code de droit économique (si des paiements ont été effectués), et demander l'application de la sanction établie à l'article VII.198 du Code de droit économique. Aussi est-il dans l'intérêt du prêteur de privilégier une forme de signature électronique pour laquelle les contestations seront très difficiles, voire impossibles. Dans ces conditions, d'aucuns pourraient considérer qu'une signature électronique qualifiée, plutôt que non-qualifiée, n'était pas nécessairement indispensable en l'espèce.

[42] Telle est d'ailleurs l'hypothèse visée par le législateur, lorsqu'il admet une signature électronique qui n'est pas qualifiée (*Doc. parl.*, Ch. repr., sess. ord. 2014-2015, n° 1300/001, p. 13). À ce sujet, voy. la contribution de H. Jacquemin et C.-R. Joly, dans le présent ouvrage.

§ 2. Document électronique

17.- Consécration du principe de non-discrimination. Le règlement eIDAS applique également le principe de non-discrimination au document électronique, en énonçant que « l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique » (art. 46).

18.- Notion de document électronique. Le document électronique est défini de manière large par le règlement eIDAS comme « tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel »[43]. La notion est plus large que l'écrit puisque le contenu peut également être sonore, visuel ou audiovisuel.

Par contre, aucune indication n'est donnée relativement aux fonctions attendues de la formalité. La proposition de la Commission du 4 juin 2012 était nettement plus ambitieuse puisqu'elle indiquait les fonctions à respecter pour que le document électronique soit jugé équivalent au document imprimé.

19.- Articulation du principe de non-discrimination avec la clause d'assimilation de l'article XII.15 du Code de droit économique. On peut se demander comment articuler, en droit belge, cette disposition avec la clause transversale particulière relative à l'écrit (figurant à l'art. XII.15, § 2, du CDE).

Lorsque l'hypothèse entre dans le champ d'application de l'article 46 du règlement (clause de non-discrimination pour le document électronique) et de l'article XII.15, § 2, du Code de droit économique (fonctions à respecter pour que le procédé soit jugé équivalent à l'écrit), aucune difficulté ne se pose. La clause de non-discrimination est d'ailleurs implicitement visée à l'article XII.15, § 2, du Code de droit économique.

Par contre, si la formalité constitue un document électronique soumis à la clause de non-discrimination de l'article 46 du règlement mais échappe au domaine d'application de l'article XII.15, § 2, du Code de droit économique (parce qu'il ne s'agit pas d'un « écrit » ou que l'hypothèse est expressément exclue par l'article XII.16 du Code de droit économique, pour les sûretés, par exemple), des discussions sont permises.

Conformément au principe de non-discrimination, le juge ne peut pas écarter le procédé. Sur ce point, le règlement eIDAS doit assurément être

[43] Art. 3, 35°, du règlement.

approuvé, dès lors qu'il n'existait pas, en droit belge, de consécration large du principe pour d'autres formalités que la signature. Le magistrat n'est toutefois pas tenu, nécessairement, de le juger équivalent au procédé « papier » correspondant. La difficulté tient au fait qu'il ne peut pas se fonder sur l'article XII.15, § 2, du Code de droit économique, et les conditions établies par celui-ci. À défaut de disposition légale réglant expressément la question en droit interne, il incomberait à la personne qui entend se prévaloir du procédé de démontrer que les fonctions traditionnellement reconnues à la formalité ont été préservées (tout en suggérant d'appliquer, par analogie, les conditions de l'article XII.15, § 2, du Code de droit économique).

SECTION 2. – Principe d'équivalence fonctionnelle

20.- **Signification et raison d'être.** Dans le courant des années quatre-vingt, parallèlement aux progrès techniques, des auteurs ont rapidement cerné les enjeux juridiques posés par le développement de l'informatique et des technologies de l'information. Ils ont esquissé les premières solutions en la matière, essentiellement sous l'angle du droit de la preuve[44]. Si d'autres solutions ont également été proposées[45], la théorie

[44] Voy. en ce sens les réflexions de B. Amory et Y. Poullet, « Le droit de la preuve face à l'informatique et à la télématique : approche de droit comparé », *D.I.T.*, 1985/5, pp. 11 et s. ; M. Fontaine, « La preuve des actes juridiques et les techniques nouvelles », *La preuve*, Actes du colloque organisé les 12 et 13 mars 1987 à l'U.C.L., pp. 1 et s. ; J. Larrieu, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? Contribution à l'étude juridique des notions d'écriture et de signature », *Cahier Lamy droit de l'informatique*, 1988, H, pp. 8 et s. ; N. Verheyden-Jeanmart, *La preuve*, Bruxelles, Larcier, pp. 233-234, nos 492-493 ; Y. Poullet, « Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve », *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*, Bruxelles, Bruylant, 1996, pp. 39 et s. ; E. Davio, « Preuve et certification sur Internet », *R.D.C.*, 1997, pp. 660 et s. ; R. Steennot, « Juridische problemen in het kader van de elektronische handel », *R.D.C.*, 1999, pp. 671 et s.

[45] Plusieurs alternatives ont été proposées en doctrine pour résoudre les difficultés posées par l'accomplissement des formes dans l'environnement numérique. Sur ces arguments, voy. B. Amory et Y. Poullet, « Le droit de la preuve face à l'informatique et à la télématique : approche de droit comparé », *op. cit.*, pp. 16-17 ; M. Fontaine, « La preuve des actes juridiques et les techniques nouvelles », *op. cit.*, pp. 16-20 ; J. Larrieu, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? Contribution à l'étude juridique des notions d'écriture et de signature », *op. cit.*, pp. 8-9 ; Fr. Labarthe, *La notion de document contractuel*, Paris, LGDJ, 1994, pp. 73 et s., nos 95 et s. ; Y. Poullet, « Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve », *op. cit.*, pp. 42-44, n° 5 ; R. Steennot, « Juridische problemen in het kader van de elektronische handel », *op. cit.*, pp. 672-673 ; D. Gobert et E. Montero, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *D.A.O.R.*, 2000, p. 18. Voy. aussi l'exposé des motifs du projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 2141/001, pp. 13-15.

[46] Comme indiqué dans le Guide pour son incorporation, « la Loi type propose [...] une nouvelle approche, parfois désignée sous l'appellation 'approche fondée sur l'équivalent fonctionnel', qui repose sur une analyse des objectifs et des fonctions de l'exigence traditionnelle de documents papier et vise à déterminer comment ces objectifs ou fonctions pourraient être assurés au moyen des techniques du commerce électronique » (*Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, New-York, Publ. des Nations Unies, 1999, p. 21, n° 16). À ce propos, voy. de E. Caprioli et R. Sorieul, « Le commerce international électronique : vers l'émergence de règles juridiques transnationales », *J.D.I.*, 2, 1997, p. 382 : « Dans leur tentative d'apporter une solution juridique à certains obstacles rencontrés par le commerce électronique, les auteurs de la loi-type se sont constamment référés aux situations juridiques connues dans le monde des documents-papier pour imaginer comment de telles situations pourraient être transposées, reproduites ou imitées dans un environnement dématérialisé ». Sur ce principe, on consultera aussi M. Demoulin, *Droit du commerce électronique et équivalents fonctionnels. Théorie critique*, coll. CRIDS, Bruxelles, Larcier, 2014.

des équivalents fonctionnels a progressivement pris corps, avant d'être consacrée, au niveau international, par la CNUDCI, dans sa loi-type sur le commerce électronique[46] (1996). Les travaux de celle-ci ont inspiré le législateur européen, puis belge.

Ce principe part du constat que les procédés mis en œuvre dans l'environnement papier pour accomplir les formes prescrites ne peuvent être reproduits comme tels lorsque le contrat est conclu par voie électronique. Si l'on souhaite que des rapports contractuels puissent être noués par ce biais, il doit être possible d'identifier les procédés à mettre en œuvre dans l'environnement numérique. Suivant la théorie des équivalents fonctionnels, on ne définit pas une exigence de forme par référence à un procédé technique particulier (le support papier pour l'écrit, le graphisme personnel et manuscrit apposé directement sur le support pour la signature, etc.) mais à la lumière des fonctions qu'elle permet de remplir (garantir la lisibilité, la pérennité, voire l'intégrité de l'information, pour l'écrit, par exemple). Deux procédés accomplis respectivement dans l'environnement traditionnel (le support papier pour l'écrit, par exemple) et dans l'environnement numérique (un document au format PDF enregistré sur un CD-ROM pour l'écrit, par exemple) sont alors jugés *équivalents* s'ils permettent de remplir les *fonctions* minimales reconnues à la formalité (l'écrit, en l'occurrence). Cette équivalence entre les procédés signifie que, sur le plan juridique, ils ont les mêmes effets et sont interchangeables. Autrement dit, la formalité prescrite est valablement accomplie dans

l'environnement numérique lorsque le procédé choisi permet d'atteindre les fonctions reconnues à l'exigence.

En droit belge, ce principe est consacré à l'article XII.15, § 1er, du Code de droit économique, aux termes duquel « toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées ». Le § 2 de cette disposition applique ensuite la théorie aux formalités rencontrées le plus souvent en pratique : l'écrit, la signature et la mention manuscrite. Encore faut-il que l'hypothèse soit couverte par l'article XII.15 (voy. notamment les exclusions figurant à l'article XII.16 du Code de droit économique).

Dans certains cas, il n'est toutefois pas nécessaire à l'interprète de la norme de se fonder sur cette théorie puisque le recours possible aux technologies de l'information est directement pris en considération par le législateur, qui désigne les formalités à accomplir au moyen de termes neutres (obligation d'accuser réception ou de transmettre des informations) ou spécialement adaptés soit à l'environnement traditionnel (le support papier), soit à l'environnement numérique (le support durable).

21.- Quid dans le règlement eIDAS ? Sans l'affirmer expressément, le règlement eIDAS applique le principe d'équivalence fonctionnelle aux principales formalités puisque, comme on le verra, les procédés susceptibles d'être utilisés sont définis par référence aux fonctions attendues d'eux. Ces fonctions sont construites par référence au procédé correspondant dans l'environnement papier, en tout cas lorsqu'il existe[47], même s'il faut constater qu'à divers égards, l'équivalence fonctionnelle est loin d'être parfaite.

On examine la signature électronique (*infra*, n° 22) et les autres services de confiance (*infra*, n° 23).

22.- Signature électronique. La signature électronique (simple) s'entend « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer »[48]. On peut difficilement considérer que le législateur européen a introduit une définition fonctionnelle de la signature électronique simple : l'acception retenue est au contraire assez tautologique, puisque la signature électronique a pour fonction de ... signer. Sans doute le législateur n'a-t-il pas voulu s'immiscer dans une analyse susceptible de révéler des différences entre les États membres. Aussi renvoie-t-il au droit interne, pour déterminer ce que « signer » signifie.

[47] Tel n'est pas le cas, par exemple, pour l'authentification de site internet.

[48] Art. 3, 10°, du règlement.

En droit privé belge, on admet généralement que les fonctions traditionnellement attendues de la signature *manuscrite* consistent à marquer l'adhésion du signataire au contenu de l'acte et à authentifier son identité[49].

La signature *électronique* fait toutefois l'objet d'une définition fonctionnelle à l'article 1322, alinéa 2, du Code civil : aux termes de cette disposition, « peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte ». Deux fonctions sont ainsi exprimées : l'imputabilité à une personne déterminée et le maintien de l'intégrité du contenu[50]. À la lumière des travaux préparatoires de la loi et des commentaires doctrinaux, on doit normalement considérer que la notion d'imputabilité couvre les fonctions traditionnellement reconnues à la signature manuscrite[51]. On peut regretter le manque de clarté de la formulation retenue

[49] Voy. H. Jacquemin, *Le formalisme contractuel : Mécanisme de protection de la partie faible*, *op. cit.*, pp. 99 et s., nos 59 et s. Cette dernière fonction est, du reste, la plus importante. À nos yeux, la fonction d'authentification est secondaire par rapport à celle-ci. L'authentification de l'origine n'est pas une fin en soi. On comprendrait d'ailleurs difficilement qu'il en soit autrement, eu égard à l'efficacité, assez réduite, du mécanisme : il n'est guère impossible de reproduire une signature manuscrite (en utilisant un calque, par exemple). En outre, la signature ne crée qu'une présomption réfragable, suivant laquelle elle émane de la personne qui s'en prétend l'auteur, et qu'il est possible de renverser. La fonction d'authentification ne doit être vue que comme une condition d'efficacité de la fonction d'adhésion : il s'agit d'un moyen entièrement dédié à la mise en œuvre de cette autre fonction. En effet, la signature ne peut manifester la volonté de son auteur de s'approprier le contenu de l'acte si ce n'est pas lui, mais un tiers, qui a accompli la formalité.

[50] Ces notions d'imputabilité et d'intégrité rappellent un attendu d'un arrêt de la Cour de cassation française du 2 décembre 1997, aux termes duquel « l'écrit [...] peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées » (Cass. fr., 2 décembre 1997, *D.*, 1998, p. 192, note D.R. Martin, *J.C.P.*, G., 1998, p. 1105, note L. Grynbaum). Soulignant ce rapprochement, voy. E. Montero, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique 'fonctionnaliste' ? », *op. cit.*, p. 188, n° 8.

[51] Voy. le rapport fait au nom de la Commission de la Justice par B. Somers, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000 (lég. 50), n° 38/008, p. 30. En doctrine, voy. E. Montero, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, p. 16 ; E. Montero, *Les contrats de l'informatique et de l'internet*, *op. cit.*, p. 247, n° 189 ; P. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », *op. cit.*, p. 114 ; L. Guinotte, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *op. cit.*, p. 558. Voy. égal. E. Montero, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique 'fonctionnaliste' ? », *Mélanges offerts à Marcel Fontaine*, Bruxelles, Larcier, 2003, p. 191, n° 9-2 : « on ne saurait donc estimer que l'imputabilité de la signature implique en tout état de cause l'adhésion au contenu. En revanche, la signature reconnue ou non contestée crée une présomption *juris et de jure* que le signataire a donné son consentement au contenu de l'acte. En principe,

(pourquoi ne pas mentionner clairement les deux fonctions et préférer une notion aussi vague et ambiguë que l'imputabilité ?) et l'ajout d'une fonction que la signature manuscrite ne permet pas d'atteindre, le maintien de l'intégrité du contenu (créant ainsi une discrimination difficilement justifiable entre la signature manuscrite et la signature électronique)[52].

On doit se demander si, pour établir ce que signifie « signer » au sens de l'article 3, 10°, du règlement eIDAS, il faut se référer aux deux fonctions de la signature manuscrite telles que reconnues par la doctrine et la jurisprudence ou aux trois fonctions de la signature électronique visée à l'article 1322, alinéa 2, du Code civil. Dès lors que l'article 1322, alinéa 2, du Code civil est d'application (parce qu'il s'agit d'une formalité probatoire ou, en passant par l'article XII.15, § 2, lorsqu'il s'agit d'une formalité requise *ad validitatem*), et sauf à ôter tout effet utile à la disposition, il paraît plus logique de décider que les trois fonctions consacrées par cette disposition doivent être préservées[53] (même si on le regrette, la disposition méconnaissant le principe d'équivalence fonctionnelle – *cf.* aussi *infra*).

Qu'en est-il des autres catégories de signatures électroniques visées par le règlement eIDAS, à savoir la signature électronique avancée[54] et la signature électronique qualifiée[55] ? Chaque procédé est une déclinaison du

on considérera que l'*animus signandi* se manifeste, par exemple, lors de la saisie, par le signataire, du code secret permettant l'activation de sa clé cryptographique. Néanmoins, il n'est pas exclu qu'un juge estime, en cas de contestation, que telle signature électronique, bien qu'imputable à telle personne, n'atteste pas son intention de s'approprier le contenu de l'acte. Même si cette condition n'est pas inscrite explicitement dans le texte, elle y figure implicitement sous la notion d'imputabilité éclairée par les travaux préparatoires, et se déduit, du reste, de la théorie générale de la signature ».

[52] Sur ce point, voy. aussi la contribution de B. Losdyck, dans le présent ouvrage.

[53] Sauf à considérer, ce qui nous paraît toutefois très artificiel, que l'article 1322, alinéa 2, vise la signature électronique, et pas la fonction de signer en tant que telle (suivant cette interprétation, on devrait se référer aux deux fonctions reconnues par la doctrine et la jurisprudence).

[54] La signature électronique avancée est « la signature électronique qui satisfait aux exigences énoncées à l'article 26 » (art. 3, 11°, du règlement eIDAS). Plus précisément, cette disposition exige que la signature satisfasse aux exigences suivantes : « a) être liée au signataire de manière univoque » ; b) « permettre d'identifier le signataire ; c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ». Ces conditions renforcent les fonctions d'identification, d'authentification et de maintien de l'intégrité du contenu de l'acte.

[55] La signature électronique qualifiée est « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique » (art. 3, 12°, du règlement). Les notions de « dispositif de création de signature électronique qualifié » et de certificat qualifié de signature électronique » sont définis par le règlement (art. 3, 15° et 23°).

précédent, soumis à des conditions complémentaires (et bénéficiant d'un régime spécifique). Aussi est-il à tout le moins requis que ces procédés soient utilisés pour « signer » (*cf.* la définition de la signature électronique simple), ce qui constitue un progrès par rapport à la loi du 9 juillet 2001. L'examen des conditions posées à l'article 4, § 4, de la loi du 9 juillet 2001 pour que la signature électronique qualifiée soit assimilée à une signature manuscrite montre en effet qu'il n'est pas expressément requis que le procédé permette de marquer l'adhésion de son auteur au contenu de l'acte[56]. En négligeant de souligner cette importante fonction de la signature, le législateur omettait de prendre en considération une différence majeure entre la signature manuscrite et le procédé de signature électronique. La fonction d'adhésion de la signature manuscrite résulte en effet de la portée symbolique que le geste revêt dans l'environnement traditionnel : en signant, on prend conscience qu'un engagement est pris et que désormais, il ne pourra en principe être délié unilatéralement sans motif et sans pénalités. Par contre, comme sous l'empire de la directive de 1999 et des dispositions de transposition (art. 4, § 4, de la loi du 9 juillet 2001 ou art. 1322, al. 2, C. civ.)[57], le règlement eIDAS exige de la signature électronique qu'elle préserve davantage de fonctions que la signature manuscrite.

S'agissant de l'authentification de l'origine, la signature électronique qualifiée offre des garanties que la signature manuscrite classique est loin d'apporter. À nos yeux, cette différence ne doit toutefois pas être critiquée. En effet, il ne s'agit pas de la seule catégorie de signature électronique susceptible d'être jugée équivalente, sur le plan des effets, à une signature manuscrite. Le cas échéant, on peut se fonder sur l'article 1322, alinéa 2, du Code civil. Et il paraît raisonnable que le législateur soit plus exigeant dans la mesure où, conformément à l'article 4, § 4, de la loi du 9 juillet 2001 ou l'article 25, § 2, du règlement eIDAS, l'assimilation est automatique (le juge ne disposant normalement d'aucun pouvoir d'appréciation).

[56] La solution est également critiquable à la lumière du considérant 20 de la directive sur la signature électronique, aux termes duquel « les signatures électroniques avancées qui sont basées sur des certificats qualifiés et qui sont créées par un dispositif sécurisé de création de signature ne peuvent être considérées comme étant équivalentes, sur le plan juridique, à des signatures manuscrites que si les exigences appliquées aux signatures manuscrites ont été respectées ». Tel n'est pas le cas en l'espèce. L'origine de la lacune réside dans le texte même de la directive, que le législateur belge a transposé littéralement. Pourtant, la première version de la proposition de directive y faisait référence (proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, *J.O.C.E.*, C. 325 du 23 octobre 1998, p. 1).

[57] À ce propos, voy. H. Jacquemin, *Le formalisme contractuel : Mécanisme de protection de la partie faible*, *op. cit.*, pp. 410 et s., n° 304.

On peut par contre regretter que la signature électronique qualifiée, la signature électronique avancée et celle régie par l'article 1322, alinéa 2, du Code civil ajoutent une fonction que la signature manuscrite ne permet pas de remplir : la fonction d'intégrité[58]. Comment expliquer que le législateur ait ajouté cette exigence ? Dans l'environnement traditionnel, l'intégrité du contenu est principalement garantie par le support papier. Dans l'environnement numérique, le support papier n'existe plus. Or, le procédé technique généralement présenté comme garantissant les fonctions de la signature électronique – la cryptographie asymétrique – permet effectivement de préserver l'intégrité des informations. Le législateur a donc exigé de la signature électronique qu'elle remplisse cette fonction. Sur le plan des principes, cette solution ne se justifie pas. Il eût été plus cohérent, selon nous, que cette fonction d'intégrité soit exigée de l'écrit[59]. En définitive, nous plaidons pour que le législateur belge amende l'article 1322, alinéa 2, du Code civil, de manière à supprimer l'exigence d'intégrité du contenu. Ce faisant, il ménagerait le principe d'équivalence fonctionnelle et simplifierait les obligations des parties qui souhaiteraient utiliser un mécanisme de signature électronique (d'autant qu'à l'analyse,

[58] Pour un regard critique sur la fonction d'intégrité, requise par l'art. 1322, al. 2, C. civ., voy. E. Montero, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, pp. 24-25 ; D. Mougenot, « La preuve », t. IV, l. II, *Rép. not.*, Bruxelles, Larcier, 2012, p. 194, n° 122-3.

[59] En outre, conformément au principe de l'équivalence fonctionnelle, il n'est pas nécessaire de trouver un procédé et un seul, qui remplirait toutes les fonctions de l'écrit ou toutes les fonctions de la signature, dans l'environnement numérique. On peut mettre en œuvre une combinaison de procédés. En pratique, rien n'empêche que la fonction d'intégrité de l'écrit soit remplie par une signature électronique. On pourrait aussi imaginer que la signature électronique ne permette pas de préserver l'intégrité du contenu mais que celle-ci soit garantie au moyen du procédé mis en œuvre au titre de l'écrit (en confiant le document à un prestataire de confiance, par exemple). En l'occurrence, cette solution ne peut toutefois être admise *de lege lata*. Il est vrai que, dans la plupart des cas, cette caractéristique critiquable de la signature électronique aura une incidence limitée dans la mesure où l'écrit et la signature sont généralement exigés conjointement. Telle est probablement la raison pour laquelle un auteur estime qu' « il eût mieux valu poser le maintien de l'intégrité comme une condition de l'acte sous seing privé électronique, sans exiger que cette intégrité résulte du mécanisme de signature. Il importe peu, en définitive, que l'intégrité de l'acte invoqué en justice soit fonction de l'écriture, du support ou de la signature. Dès lors que l'intégrité de l'acte est attestée et que le mécanisme de signature utilisé par les parties permet de les identifier et d'exprimer leur adhésion, faut-il dénier à ce dernier la qualité de signature au motif qu'il n'établit pas, par lui-même, le maintien de l'intégrité du contenu de l'acte ? » (E. Montero, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique 'fonctionnaliste' ? », *op. cit.*, p. 192, n° 10). En définitive, la fonction d'intégrité doit donc être garantie, peu importe qu'on l'attribue à l'écrit ou à la signature. Globalement, toutes les fonctions de l'écrit et de la signature seront préservées. Dans certains cas, cependant, l'écrit ne doit pas nécessairement être signé.

mais de manière critiquable, la jurisprudence belge néglige de vérifier si la fonction a effectivement été préservée[60]).

23.- Autres services de confiance. Pour les autres services de confiance, une distinction peut être faite suivant qu'il existe (ou pas) un équivalent dans l'environnement traditionnel.

L'horodatage électronique vise « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant »[61]. Deux fonctions sont ainsi requises du procédé d'horodatage électronique : indiquer la date et l'heure avec précision et garantir l'intégrité des données auxquelles se rapportent cette date et cette heure[62]. Le mécanisme ne connaît pas, en tant que tel, d'équivalent dans l'environnement « papier ». On peut soit se fonder sur l'une des hypothèses visées à l'article 1328 du Code civil[63], qui donne date certaine aux actes sous seing privé, soit établir un acte authentique. À défaut, la date de l'envoi recommandé à la poste peut être invoqué mais elle constitue tout au plus une présomption de l'homme.

De même, la délivrance de certificats d'authentification de site internet ne connaît pas d'équivalent dans l'environnement papier (où, à la différence de l'horodatage, le problème ne se rencontre même pas en tant que tel, en l'absence de site internet – aussi l'application de la théorie des équivalents fonctionnels ne se pose-t-elle pas). Il s'agit de l' « attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré »[64]. L'objectif est clairement de lutter contre le *phishing* ou d'autres pratiques frauduleuses semblables. Le cachet électronique n'a pas non plus d'équivalent dans

[60] Voy. C. trav. Bruxelles, 11 octobre 2013 et 14 février 2014, *R.D.T.I.*, 2014/56, p. 115 et la note de J.-B. Hubin, « Signature scannée : quand une technologie simple confronte le juriste à des questions complexes ». Dans l'arrêt du 11 octobre 2013, la Cour du travail avait bien noté l'exigence du maintien de l'intégrité. Pourtant, dans l'arrêt du 14 février 2014 (la Cour ayant posé des questions aux parties et ordonné une réouverture des débats), elle accorde des effets juridiques à une signature scannée sans vérifier que la fonction a effectivement été préservée.

[61] Art. 3, 33°, du règlement.

[62] Voy. art. 41, § 2, du règlement, qui énonce clairement ces fonctions et présume qu'elles sont remplies dans l'hypothèse de l'horodatage électronique qualifié.

[63] Etant entendu que l'horodatage électronique, même qualifié, ne permet pas, à lui seul, de donner date certaine à un document au sens de l'article 1328 du Code civil (en ce sens, voy. le futur art. XII.25, § 10, du CDE, tel qu'introduit par l'article 7 de l'avant-projet de loi).

[64] Art. 3, 38°, du règlement.

l'environnement papier, une personne physique intervenant généralement en tant qu'organe de la personne morale.

Par contre, pour le service d'envoi recommandé électronique, on trouve un procédé correspondant dans l'environnement papier. Le service d'envoi recommandé électronique est le « service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée »[65]. Le règlement eIDAS liste ainsi les fonctions attendues du service d'envoi recommandé électronique : preuve de l'envoi et de la réception des données et maintien de leur intégrité (puisqu'elles doivent être protégées des risques de perte, de vol ou de modification). On regrette par contre que les fonctions attendues du recommandé électronique ne correspondent pas parfaitement à celles du recommandé papier traditionnel et sont en réalité plus nombreuses[66].

SECTION 3. – Principe de neutralité technologique

24.- Notion. Le principe *de neutralité technologique* est à la base de toutes les interventions normatives en lien avec l'accomplissement des formes dans l'environnement numérique[67]. Suivant celui-ci, les dispositions normatives doivent rester neutres et ne pas désigner expressément une technologie déterminée : eu égard à la rapidité des progrès scientifiques et techniques, il est en effet hautement probable que cette technologie devienne à brève échéance totalement obsolète. Il faudrait dès lors modifier les textes normatifs continuellement, pour qu'ils correspondent aux standards techniques minimaux, de nature à maintenir le niveau de sécurité requis.

25.- Quid dans le règlement eIDAS ? Le principe est consacré par les considérants n^{os} 26 et 27 du règlement eIDAS : après avoir constaté que

[65] Art. 3, 36°, du règlement.

[66] Sur les fonctions du recommandé, voy. E. Montero, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées », *Commerce électronique : de la théorie à la pratique*, coll. Cahier du CRID, n° 23, Bruxelles, Bruylant, 2003, pp. 75 et s. Comp. D. Gobert, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution », , *op. cit.*, pp. 47-48, qui appuie cette solution.

[67] Voy. le considérant n° 8 de la directive sur la signature électronique ou la loi type de la CNUDCI de 2001 sur les signatures électroniques et le Guide pour son incorporation, New York, Publ. des Nations Unies, 2002, p. 35, n° 82. Voy. aussi, plus récemment, les considérants n^{os} 26 et 27 du règlement eIDAS.

« vu la rapidité de l'évolution technologique, le présent règlement devrait consacrer une approche qui soit ouverte aux innovations », il est indiqué que « le présent règlement devrait être neutre du point de vue de la technologie. Les effets juridiques qu'il confère devraient pouvoir être obtenus par tout moyen technique, pour autant que les exigences posées par le présent règlement soient satisfaites ».

La consécration de ce principe doit assurément être approuvée, même s'il paraît clair – mais ce n'est pas contestable en soi – qu'en posant les conditions applicables notamment à la signature, le législateur avait en tête les procédés créés au moyen de la cryptographie asymétrique.

Les stipulations figurant dans le règlement formulent les exigences en termes de mesures à prendre et fonctions à préserver. Le texte ne dit donc pas, par exemple, qu'il faut respecter la norme ISO unetelle ou recourir à la cryptographie asymétrique. Compétence est toutefois donnée à la Commission européenne d'établir, au moyen d'actes d'exécution, les numéros de référence de normes (techniques ou organisationnelles) à respecter[68]. Le règlement préserve ainsi le principe de neutralité technologique, tout en permettant au secteur de disposer d'informations claires quant aux exigences techniques auxquelles ils sont soumis (et que la Commission veillera à actualiser si nécessaire). Le règlement prévoit d'ailleurs que le prestataire est présumé respecter les exigences que ses dispositions énoncent lorsque les normes en question sont respectées.

CHAPITRE III. Être ou ne pas être qualifié ?

SECTION 1. – Considérations générales

26.- *Summa divisio*. Le règlement établit une *summa divisio* entre, d'une part, les prestataires de services de confiance (PSC) qualifiés et les services de confiance (SC) qualifiés, d'autre part, les prestataires de service de confiance non qualifiés et les services de confiance non qualifiés.

[68] Voy. les art. 24, § 5 (exigences applicables aux PSC qualifiés), 27, § 4 (signatures électroniques dans les services publics), 28, § 6 (certificats qualifiés de signature électronique), 29, § 2 (dispositifs de création de signature électronique qualifiés), 32, § 3 (validation des signatures électronique qualifiées), 33, § 2 (services de validation qualifié des signatures électroniques qualifiées), 34, § 2 (services de conservation qualifié des signatures électroniques qualifiées), 37, § 4 (cachets électroniques dans les services publics), 38, § 6 (certificats qualifiés de cachet électronique), 42, § 2 (établissement du lien entre la date et l'heure et les données, et les horloges exactes, en matière d'horodatage électronique), 44, § 2 (processus d'envoi et de réception des données en matière de service d'envoi recommandé électronique) et 45, § 2 (certificats qualifiés d'authentification de sites internet).

Les notions de « prestataire de service de confiance » et de « service de confiance » ont déjà été présentées (*supra*, n° 6).

Comme on le verra, des conditions particulièrement rigoureuses doivent être observées par les prestataires s'ils veulent obtenir le statut de qualifié et lancer leur activité (*infra*, n° 32). Parallèlement dans l'exercice même de leur activité, de nombreuses obligations leur sont imposées, en lien avec les services de confiance qu'ils délivrent (*infra*, n° 33). Il en résulte des contraintes techniques et organisationnelles importantes ainsi qu'une charge administrative et financière très lourde. Autrement dit, il est hautement probable qu'au sein des États membres, voire au niveau de l'Union, de tels prestataires soient finalement peu nombreux.

Le respect de ces conditions donne lieu à l'application d'un régime juridique plus favorable aux parties utilisatrices du service de confiance : les effets juridiques des services de confiance qualifiés leur permettent de bénéficier d'une clause d'assimilation ou d'une présomption légale (*infra*, n° 35) ; le prestataire qualifié est présumé avoir agi intentionnellement ou par négligence (*infra*, n° 36) ; les service qualifiés sont reconnus en tant tels dans tous les États membres (*infra*, n° 37). Sur ce point, l'objectif du règlement est clair : aux termes du considérant n° 28, « pour accroître, en particulier, la confiance des petites et moyennes entreprises (PME) et des consommateurs dans le marché intérieur et pour promouvoir l'utilisation des services et produits de confiance, les notions de service de confiance qualifié et de prestataire de service de confiance qualifié devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis ».

Au contraire, les services de confiance non-qualifiés bénéficient d'effets juridiques soumis à l'aléa de la preuve (et aucune présomption ne peut être invoquée en termes de responsabilité). Le risque existe donc que la preuve ne puisse pas être apportée (même si, très clairement, et suivant le procédé utilisé, il peut fort bien ne pas se réaliser).

Tout dépend en définitive du risque que l'on est prêt à assumer, lorsque l'on recoure à un service de signature, de cachet, de recommandé ou d'horodatage électronique. Si l'enjeu financier – ou le risque en général – est faible, sans doute n'est-il pas requis de déployer l'artillerie lourde en surprotégeant l'opération : pour donner un exemple concret, on ne passe pas devant le notaire pour constater l'achat de quelques meubles de jardin entre particuliers (même si, sur le plan probatoire, la sécurité juridique est renforcée en recourant à l'acte authentique plutôt qu'à l'acte sous seing privé). Par contre, s'il s'agit d'un contrat portant sur plusieurs millions d'euros et que la date de signature est primordiale, on sera bien avisé de recourir à un service d'horodatage et de signature électroniques qualifiés.

27.- **Organe de contrôle.** Pour s'assurer que les prestataires de services de confiance – spécialement les PSC qualifiés – sont dignes... de la confiance que le règlement leur accorde, celui-ci impose la désignation d'un « organe de contrôle » par les États membres[69]. Son rôle est précisé par l'article 17 du règlement. Suivant l'avant-projet de loi, cet organe de contrôle est créé au sein du SPF Économie, PME, Classes moyennes et énergie[70].

Parmi d'autres, ils sont tenus de réaliser des contrôles *a priori* et *a posteriori* des PSC qualifiés (et des SC qualifiés qu'ils fournissent). Si nécessaire, ils doivent également prendre des mesures de contrôle *a posteriori* à l'égard des PSC non qualifiés (et des SC qu'ils fournissent), s'ils sont informés que les dispositions du règlement seraient méconnues[71].

Le règlement pose aussi les bases d'une assistance mutuelle entre les organes de contrôle des États membres[72].

SECTION 2. – Régime harmonisé pour tous les PSC, qualifiés ou non-qualifiés

§ 1. Conditions

28.- **Traitement des données à caractère personnel.** L'article 5 du règlement, dont l'application ne se limite pas aux services de confiance, exige que les traitements de données à caractère personnel se fassent conformément à la directive 95/46/CE. Lorsqu'il sera applicable, on aura également égard au projet de règlement général sur la protection de données.

En Belgique, en cas d'utilisation de la carte d'identité électronique, on sera particulièrement attentif aux exigences figurant dans la loi du 8 août 1983 organisant un registre national des personnes physiques, en particulier, à l'article 8, aux termes duquel « l'autorisation d'utiliser le numéro d'identification du Registre national est octroyée par le comité sectoriel

[69] L'art. 17, § 1er, du règlement exige en effet qu'ils désignent « un organe de contrôle établi sur leur territoire ou, d'un commun accord avec un autre État membre, un organe de contrôle établi dans cet autre État membre. Cet organe est chargé des tâches de contrôle dans l'État membre qui a procédé à la désignation.

Les organes de contrôle sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour l'exercice de leurs tâches ».

[70] Voy. la définition figurant au futur article I.18, 16°, du CDE, telle qu'introduite par l'article 2 de l'avant-projet de loi.

[71] Sur ce point, voy. aussi le considérant n° 36 du règlement.

[72] Art. 18 du règlement.

du Registre national visé à l'article 15, aux autorités, aux organismes et aux personnes visés à l'article 5, alinéa 1er. Le comité sectoriel envoie dans les trente jours après sa décision une copie de celle-ci au ministre de l'Intérieur et au ministre de la Justice. (...) »[73].

29.- **Accessibilité aux personnes handicapées.** L'article 15 du règlement prévoit que « dans la mesure du possible, les services de confiance fournis, ainsi que les produits destinés à un utilisateur final qui servent à fournir ces services, sont accessibles aux personnes handicapées ». En ce sens, le considérant n° 29 indique que l'évaluation de la faisabilité doit notamment se faire à l'aune de considérations d'ordre technique et économique.

30.- **Exigences en matière de sécurité.** L'article 19, § 1er, du règlement impose aux prestataires de prendre « les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents ».

En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur le service fourni ou sur les données à caractère personnel qui y sont conservées, une obligation de notification pèse sur les prestataires, vis-à-vis de l'organe de contrôle[74] et, le cas échéant, des bénéficiaires des services de confiance concernés[75], conformément à l'article 19, § 2, du règlement. La notification doit intervenir dans les meilleurs délais. Pour la notification à l'organe de contrôle, le règlement impose un délai de 24 heures prenant cours à partir de leur connaissance par le prestataire de confiance. On ne négligera pas la charge (administrative et financière) que représente une telle obligation, particulièrement si le prestataire a plusieurs milliers (ou millions, pour des multinationales du secteur des

[73] Sur ce point, voy. la contribution de Cécile de Terwangne et Elise Degrave, dans le présent ouvrage.

[74] Il peut aussi s'agir d'autres organes compétents (le règlement cite l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, autrement dit la Commission de protection de la vie privée, pour la Belgique).

[75] Cette exigence ne s'impose que « lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni ».

télécoms, par exemple) de clients. Le cas échéant, il peut être requis d'informer les organes de contrôles d'autres États membres et l'ENISA, voire le public en général, si l'organe de contrôle décide qu'il est dans l'intérêt public de procéder à une telle divulgation[76].

§ 2. Effets

31.- **Principe de non-discrimination.** Le règlement eIDAS applique le principe de non-discrimination à tous les services de confiance, qu'ils soient qualifiés ou pas (*cf. supra*, nos 10 et s.).

Cela signifie que l'effet juridique ou la recevabilité de ces services de confiance comme preuve en justice ne peuvent pas être refusés au seul motif qu'ils se présentent sous une forme électronique ou qu'ils ne satisfont pas aux exigences du service de confiance qualifié correspondant.

SECTION 3. – Régime différencié pour les services de confiance qualifiés et non qualifiés

§ 1. Conditions

32.- **Conditions pour lancer un service de confiance qualifié.** Lorsqu'un prestataire de services de confiance veut fournir des SC qualifiés et obtenir le statut de PSC qualifié, il doit préalablement obtenir une autorisation de l'organe de contrôle. La procédure est décrite à l'article 21 du règlement.

Le régime est ainsi diamétralement opposé à celui qui prévalait sous l'empire de la directive de 1999 en matière de signature électronique puisqu'elle interdisait aux États membres de soumettre les prestataires de services de certification à un régime d'autorisation préalable[77]. Le système mis en place par le règlement offre davantage de garanties quant au prestataire même si on peut craindre que cette exigence ait un effet dissuasif. Conformément aux lois de transpositions de la directive de 1999, les prestataires fournissant des services de signature électronique qualifiée étaient très rares. *A fortiori*, avec cette exigence additionnelle, on peut sérieusement douter qu'ils soient plus nombreux...

[76] Art. 19, § 2, du règlement.

[77] Art. 3, § 1er, de la directive 1999/93/CE. Un régime volontaire d'accréditation pouvait toutefois être organisé (art. 3, § 2, de la directive).

La notification soumise par le prestataire à l'organe de contrôle doit être accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité[78].

C'est principalement sur cette base que l'organe de contrôle vérifiera le respect des exigences du règlement et, en cas d'appréciation positive, leur accordera le statut de « qualifié » (normalement dans un délai de trois mois à compter de la notification[79]).

Il est primordial que toutes les parties prenantes (les parties utilisatrices, les prestataires et les autorités publiques compétentes) sachent avec certitude qui sont les prestataires qualifiés. Aussi incombe-t-il aux États membres d'établir, de publier et de mettre à jour des listes de confiance[80]. De son côté, la Commission met à la disposition du public les informations permettant de consulter ces listes (et de connaître l'organisme chargé de les publier). Cette publication sur une liste de confiance est importante puisque les prestataires ne peuvent fournir des services dits « qualifiés » qu'à partir du moment où leur statut est indiqué sur celles-ci[81]. À cet instant, ils peuvent également utiliser le label de confiance de l'Union[82] et l'apposer, par exemple, sur leur site internet ou tout autre document promotionnel.

33.- Exigences applicables aux PSC qualifiés (dans l'exercice de leur activité). L'article 24 du règlement liste les nombreuses exigences applicables, de manière générale, aux PSC qualifiés.

Les prestataires qui délivrent des certificats qualifiés doivent vérifier l'identité et, éventuellement, les attributs de la personne physique ou morale à laquelle celui-ci est délivré[83]. Des règles encadrent également l'établissement et la mise à jour d'une base de données relative aux

[78] La notion est définie l'art. 3, 18°, du règlement.

[79] Le règlement autorise toutefois l'organe de contrôle à prolonger le délai pour autant qu'il informe le prestataire, en lui indiquant les raisons du retard et le délai nécessaire pour achever la mission.

[80] Art. 22 du règlement.

[81] Art. 21, § 3, du règlement.

[82] Art. 23 du règlement. Voy. le règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés, *J.O.*, L. 128 du 23 mai 2015, ainsi que la décision d'exécution (UE) 2015/1505 de la Commission du 8 septembre 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, *J.O.*, L. 235 du 9 septembre 2015.

[83] Art. 24, § 1er, du règlement. Cette disposition indique par qui et comment cette vérification peut être faite, conformément au droit national.

certificats, ainsi que la révocation éventuelle de ceux-ci (l'opération de révocation en tant que telle et l'information qui doit en être donnée).

Le règlement énumère aussi, au § 2 de l'article 24, diverses obligations tenant aux obligations d'information vis-à-vis de l'organe de contrôle (a) ou des parties utilisatrices (d), aux compétences de leur personnel et sous-traitants éventuels (b), aux ressources financières et aux assurances (c), à la fiabilité et à la sécurité des systèmes et produits mis en place (d à g), à l'archivage des informations pertinentes concernant les données délivrées et reçues (h), ou à la continuité de leurs activités, par la mise en place d'un plan actualisé d'arrêt (i).

En complément de ces exigences d'ordre général, il faut ajouter les conditions propres à certains services de confiance qualifiés. En matière de signature (et de cachet), le règlement détermine les exigences relatives aux certificats qualifiés de signature (ou de cachet) électronique[84], aux dispositifs de création de signature électronique qualifiés (les exigences applicables à ceux-ci, la certification des dispositifs et la publication de ceux-ci)[85], ainsi qu'à la validation et la conservation des signatures (et des cachets) électroniques qualifiés[86]. Des conditions figurent également aux annexe I à III du règlement.

Le règlement impose aux PSC qualifiés de faire l'objet d'un audit dont les résultats doivent être transmis à l'organe de contrôle[87]. Il doit être réalisé tous les 24 mois, au frais du prestataire, par un organisme d'évaluation de conformité. Cet audit peut aussi être demandé par l'organisme de contrôle à tout moment[88]. L'organe de contrôle peut être amené à imposer au prestataire de corriger certains manquements aux exigences prévues par le règlement et, à défaut de réponse satisfaisante, la sanction peut aller jusqu'à priver le prestataire ou le service concerné du statut de « qualifié »[89].

On aura aussi égard au futur article XII.36 du Code de droit économique[90], qui règle l'arrêt des activités d'un prestataire de service de confiance qualifié et la reprise éventuelle des activités par un autre prestataire.

[84] Art. 28 pour la signature et art. 38 pour le cachet.

[85] Art. 29-31 pour la signature et art. 39 pour le cachet.

[86] Art. 32-34 pour la signature et art. 40 pour le cachet.

[87] Art. 20, § 1er, du règlement.

[88] Art. 20, § 2, du règlement.

[89] Art. 20, § 3, du règlement.

[90] Introduit par l'article 23 de l'avant-projet de loi.

§ 2. Effets

34.- Des avantages de la qualification. On observe des différences importantes – et logiques – entre les effets attachés aux services de confiance qualifiés ou non qualifiés, en termes de clause d'assimilation ou de présomption (*infra*, n° 35), de responsabilité (*infra*, n° 36) et de reconnaissance internationale (*infra*, n° 37).

35.- Clause d'assimilation ou présomption pour les services de confiance qualifiés. Les services de confiance qualifiés bénéficient du principe d'assimilation ou d'une présomption légale ayant pour effet de renverser la charge de la preuve.

Aux termes de l'article 25, § 2, du règlement, « l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite ». *A priori*, le juge ne dispose d'aucune marge d'appréciation et il doit assimiler le procédé à une signature manuscrite. D'après nous, il doit rester possible d'administrer la preuve contraire.

Pour d'autres services de confiance, le règlement présume – de manière réfragable – que les fonctions reconnues à la formalité (et expressément mentionnées) sont atteintes. Tel est le cas pour le cachet électronique qualifié[91] (présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié), l'horodatage électronique qualifié[92] (présomption d'exactitude de la date et de l'heure qu'il indique d'intégrité des données auxquelles se rapportent cette date et cette heure), le service d'envoi recommandé électronique qualifié[93] (présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié). Pour le cas plus particulier de l'authentification de site internet, aucune présomption n'est établie.

Qu'en est-il des services de confiance qui ne sont pas qualifiés (et qui ne bénéficient donc pas de la clause d'assimilation ou de la présomption) ?

Sous peine de méconnaître le principe de non-discrimination consacré par ailleurs (et qui interdit de priver d'effet juridique les services de confiance qui ne sont pas qualifiés), il faut admettre que les parties utilisatrices aient la possibilité de démontrer que la signature, le cachet, l'horodatage ou le service d'envoi recommandé respectent les fonctions

[91] Art. 35, § 2, du règlement.
[92] Art. 41, § 2, du règlement.
[93] Art. 43, § 2, du règlement.

reconnues à chaque procédé, de manière à convaincre le juge de leur donner des effets juridiques.

Les États membres retrouvent sur ce point leur marge de manœuvre de manière à préciser les fonctions attendues de chaque formalité[94]. Pour la signature électronique, par exemple, c'est le rôle joué par l'article 1322, alinéa 2, du Code civil et on peut supposer qu'il sera conservé par le législateur.

Peut-être introduira-t-il des dispositions comparables pour les autres services de confiance. La démarche ne nous paraît toutefois pas indispensable dans la mesure où, contrairement à la signature, le règlement veille à indiquer clairement les fonctions attendues de ces services dans la définition qui leur est donnée. Une clause transversale générale indiquant qu'il incombe à la partie utilisatrice de démontrer que les fonctions ainsi énoncées sont remplies pour bénéficier des effets sur le plan probatoire (ou autre, le cas échéant), devrait être suffisante.

On note encore que la signature électronique avancée et le cachet électronique avancé peuvent être reconnus, moyennant certaines conditions, si un État membre exige ce type de signature (le cas échéant qui repose sur un certificat qualifié) pour utiliser un service en ligne offert par un organisme du secteur public ou pour l'utiliser au nom de cet organisme[95]. *A fortiori*, dans ce cas, les signatures ou cachets électroniques présentant un niveau de sécurité plus élevé (tels que la signature ou le cachet électroniques qualifiés) se voient reconnaître les mêmes effets. Cette disposition tend à compliquer le régime mis en place (puisqu'il crée une autre catégorie de signature électronique) : le considérant n° 50 du règlement le justifie cependant par le fait que « les autorités compétentes dans les États membres utilisent actuellement différents formats de signature électronique avancée pour signer électroniquement leurs documents ».

36.- Responsabilité. Aux termes de l'article 13, § 1er, du règlement, « [...] les prestataires de service de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement ».

Le règlement instaure un régime probatoire plus favorable aux parties utilisatrices de services fournis par des PSC qualifiés puisque, dans

[94] S'agissant de la signature, voy. le considérant n° 49 : « il appartient au droit national de définir l'effet juridique produit par les signatures électroniques, à l'exception de l'exigence prévue dans le présent règlement selon laquelle l'effet juridique d'une signature électronique qualifiée devrait être équivalent à celui d'une signature manuscrite ».
[95] Art. 27 et 37 du règlement.

ce cas, le prestataire est présumé avoir agi intentionnellement ou par négligence[96]. Pour les autres prestataires, c'est le droit commun qui s'applique et il incombe à la victime de prouver que le prestataire a agi intentionnellement ou par négligence[97].

On note qu'il est permis aux prestataires de services de confiance de poser des limites à l'utilisation des services fournis (indiquer par exemple que le service de signature ou d'horodatage électronique n'est pas garanti pour des montants supérieurs à 1.000.000 euros ou dans certaines matières – comme des paiements). Cette limite – et l'exonération limitative de responsabilité qui en découle – sera étroitement liées aux garanties obtenues par les prestataires auprès de leurs compagnies d'assurance (tenant compte des risques financiers qu'ils sont prêts à assumer)[98]. Encore faut-il, comme le rappelle l'article 13, § 2, du règlement, que les clients soient dûment informés, au préalable, de telles limites, et qu'elles puissent être reconnues par des tiers.

37.- Reconnaissance mutuelle au sein de l'Union. Parmi les objectifs du règlement figure le bon fonctionnement du marché intérieur. Il doit se traduire par une libre prestation des services de confiance sur le territoire de l'Union (dans le chef des prestataires qui les fournissent et des parties utilisatrices qui y recourent). Concrètement, il faut permettre à un client belge qui conclut un contrat avec une entreprise française d'utiliser un procédé d'horodatage électronique fourni par une entreprise finlandaise.

En ce sens, le règlement consacre un principe de reconnaissance mutuelle de certains services de confiance qualifiés. Il énonce ainsi « la signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les États membres »[99]. Des clauses similaires sont introduites pour les cachets électroniques qualifiés[100], l'horodatage électronique qualifié[101]. Curieusement, rien n'est prévu pour le service d'envoi recommandé électronique qualifié ou la délivrance de certificats qualifiés d'authentification de sites internet.

Qu'en est-il des services de confiance non-qualifiés ou des deux services de confiance qualifiés qui ne bénéficient pas de la clause de reconnaissance mutuelle ? Le principe de marché intérieur tel que consacré à l'article 4 du règlement leur est applicable. En son § 1er, cette disposition

[96] Art. 13, § 1er, al. 3, du règlement.
[97] Art. 13, § 1er, al. 2, du règlement.
[98] Sur ce point, voy. le considérant n° 37 du règlement.
[99] Art. 25, § 3, du règlement.
[100] Art. 35, § 3, du règlement.
[101] Art. 41, § 3, du règlement.

interdit en effet de restreindre « la fourniture de services de confiance, sur le territoire d'un État membre, par un prestataire établi dans un autre État membre, pour des raisons qui relèvent des domaines couverts par le présent règlement ». Quant au § 2, il autorise les services de confiances conformes au règlement à circuler librement au sein du marché intérieur.

Conclusion

38.- Sécurité juridique et technique renforcée. Le règlement eIDAS vise à instaurer ainsi un climat de confiance propice au développement du commerce électronique.

De manière générale, le règlement doit être approuvé, en ce qu'il renforce la sécurité juridique et technique concernant les services de confiance (sous réserve néanmoins des services d'archivage électronique, dont on regrette l'absence de cadre normatif au niveau européen).

Il faut toutefois reconnaître que le régime mis en place est parfois très complexe (et peu lisible). Il fait aussi la part belle aux prestataires de service de confiance qualifiés et aux services de confiance qualifiés, même si l'on peut craindre qu'au final, les prestataires intéressés restent très rares.

39.- En pratique... Les objectifs poursuivis par le règlement ne seront atteints que si le marché – on vise tant les prestataires que les destinataires des services – se montre plus réactif que lors de l'adoption de la directive sur la signature électronique, il y a 15 ans. Il faut en effet espérer qu'ils soient davantage convaincus par les dispositions du règlement et, respectivement, offrent ou utilisent les services de confiance encadrés par celui-ci.

Sans doute des initiatives pourraient-elles être prises par les pouvoirs publics pour promouvoir – sans nécessairement imposer – le recours à ces services et, en quelque sorte, amorcer la machine...

À défaut, on peut craindre – et regretter – que ces dispositions restent lettre morte et soient une nouvelle occasion manquée de renforcer la confiance et développer les transactions en ligne.